[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/24

[12] 发明专利申请公开说明书

[21] 申请号 02111251.7

[43] 公开日 2003 年 10 月 15 日

[11] 公开号 CN 1449157A

[22] 申请日 2002.3.30 [21] 申请号 02111251.7
[71] 申请人 深圳市中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法律部
[72] 发明人 李 进
权利要求书 2 页 说明书 5 页 附图 3 页

[54] 发明名称 一种网络管理系统和方法

[57] 摘要

本发明公开了一种网络管理系统和方法，由客户端、应用服务器、被管对象组成网络管理系统的三层结构；应用服务器和被管对象之间的通信使用网络管理通信协议，都位于安全网络环境中；客户端通过互联网采用适合于互联网环境的通信协议与应用服务器通信；应用服务器负责解析客户端的报文请求，并转化为相应的网络管理协议的请求，发送到被管对象，并将被管对象的相关数据转化为相应的报文发送到客户端。采用本发明的网络管理系统和方法，能够增强互联网环境中被管理设备的安全性，适用于数据通信特别是互联网环境下的网络管理领域。

ISSN1008-4274

1. 一种网络管理系统，其特征在于，所述网络管理系统包括：客户端、应用服务器、被管对象；应用服务器和被管对象之间的通信使用网络管理通信协议，都位于安全网络环境中；客户端通过互联网采用适合于互联网环境的通信协议与应用服务器通信；应用服务器负责解析客户端的报文请求，并转化为相应的网络管理协议的请求，发送到被管对象，并将被管对象的相关数据转化为相应的报文发送到客户端。

2. 根据权利要求 1 所述的一种网络管理系统，其特征在于，所述被管对象是被管设备或是被管设备代理。

3. 根据权利要求 1 所述的一种网络管理系统，其特征在于，所述客户端包括：协议处理器，负责处理客户端与应用服务器之间的协议处理；流处理器，负责与应用服务器建立连接。

4. 根据权利要求 1 所述的一种网络管理系统，其特征在于，所述应用服务器包括：动态页面引擎，实现应用服务器端的 WWW 服务；应用程序接口，用于实现应用服务器与被管设备的通信。

5. 根据权利要求 1 或 2 或 3 或 4 所述的一种网络管理系统，其特征在于，所述应用服务器和所述被管对象之间的网络管理通信协议是简单网络管理协议 SNMP、电信网管协议或 Q3 协议。

6. 根据权利要求 1 或 2 或 3 或 4 所述的一种网络管理系统，其特征在于，所述客户端与所述应用服务器之间的通信协议是 HTTP 协议、简单邮件传输协议、网络新闻传输协议或简单对象访问协议 SOAP。

7. 根据权利要求 1 或 2 或 3 或 4 所述的一种网络管理系统，其特征在于，所述

客户端与应用服务器之间设置防火墙。

8．一种网络管理方法，其特征在于，实现步骤为：

1）客户端选择与应用服务器通信的协议处理器；

2）所述协议处理器实例化出一个流处理器供所述客户端使用；

3）所述客户端将对被管对象网络管理的相关信息发送到所述流处理器；

4）所述流处理器建立与所述应用服务器的通信联系，并将接收到的客户端信息转化成协议可传送的报文并发送到所述应用服务器；

5）所述应用服务器以多线程的方式对所述客户端的所有请求分别响应；

6）所述应用服务器分析接收到的报文信息，并调用网络管理通信协议的应用程序接口；

7）所述应用服务器通过网络管理协议完成与所述被管对象的消息交互，并将结果通过网络管理通信协议的应用程序接口和所述流处理器返回客户端。

一种网络管理系统和方法

所属技术领域：

本发明涉及一种数据通信的网络管理领域，特别是在互联网环境中的网络管理系统和方法。

背景技术：

随着网络、通讯和计算机软件技术的发展，大多数企业面临全球化竞争。现代企业的计算机系统包括各种设备，并分布在全国甚至世界各地。这就需要有一种软件可以方便的通过互联网管理和监测各地的计算机系统以及各种设备。而大多数企业现有的网络管理软件多数都是基于传统的客户机/服务器模式。这种模式在互联网盛行的今天有如下的问题：

1、以基于简单网络管理协议（SNMP）为基础的网络管理系统为例。由于SNMP是TCP/IP的应用层的协议之一，所以客户端为了可以管理相应的设备，可能需要正确配置网关或者路由才可以通过SNMP进行网络管理。首先对于一般的用户来说，正确配置网关或者路由可能是比较困难的；其次在互联网环境中，客户端到被管理设备必须可以建立起用户数据报协议（UDP）的连接，这在互联网环境中是不安全的。以其它的网络协议为基础的网管系统更加不适合互联网的网络环境。

2、为了安全起见，大多数网络中的设备需要在设备代理端配置网管系统的主机地址。如果在设备配置表中没有配置该网管系统的主机地址，设备代理是不处理网管系统的请求。网管系统也就不能进行相关网络管理的操作了。在互联网环境中，大多数客户端的IP地址是由ISP动态分配的，IP地址的不确定性导致网络管理的不可行。在某些情况下，客户端可能需要经过防火墙才能访问设备代理。这时候，设备代理和网管系统不能直接建立连接。这对于基于客户端/服务器模式的网络管理来说是很难实现互联网环境的网络管理。

3、从安全的角度来说。如果网络设备和互联网之间没有隔离层，是会存在安全隐患的。而且许多的网管协议中，安全考虑是比较少的。以SNMP协议为例，在SNMP协议的第一、第二版中都没有对安全提出完整的解决方案，而只是通过团体串来进行权限的简单控制。如果设备代理暴露在互联网环境中，别有

用心的黑客可以通过网络报文分析工具分析 UDP 报文就可以知道团体串的内容。如果网络设备的网络管理信息库中存储有敏感数据，这将是非常大的安全隐患。简单网络管理通信协议第三版虽然有了较好的解决方案，但是实现起来比较复杂，而且现有的大多数的设备并不支持。

而且由于互联网环境的网络管理系统必须保证安全，所以被管理设备必须放置于安全网络中，互联网用户的访问必须经过防火墙的过滤来保证安全。现有的网络管理系统和方法还不能很好的解决这方面的问题。

发明内容：

本发明克服了现有网络管理系统的不足，提出了一种在互联网环境中的安全网络管理系统。

本发明还提出了一种网络管理方法，客户端能够通过互联网，并透过防火墙对被管设备进行安全的网络管理。

本发明所述的网络管理系统包括：客户端、应用服务器、被管对象；应用服务器和被管对象之间的通信使用网络管理通信协议，都位于安全网络环境中；客户端通过互联网采用适合于互联网环境的通信协议与应用服务器通信；应用服务器负责解析客户端的报文请求，并转化为相应的网络管理协议的请求，发送到被管对象，并将被管对象的相关数据转化为相应的报文发送到客户端。

所述被管对象是被管设备或是被管设备代理。

所述应用服务器和被管对象之间的网络管理通信协议是简单网络管理协议（SNMP）、电信网管协议或 Q3 协议。

所述客户端与应用服务器之间的通信协议是 HTTP 协议、简单邮件传输协议、网络新闻传输协议或 SOAP 简单对象访问协议。

所述客户端与应用服务器之间可以设置防火墙，确保安全网络环境的安全。

本发明提出的一种网络管理方法，其实现步骤如下：

1）客户端选择与应用服务器通信的协议处理器；

2）协议处理器实例化出一个流处理器供客户端使用；

3）客户端将对被管对象网络管理的相关信息发送到流处理器；

4）流处理器建立与应用服务器的通信联系，并将接收到的客户端信息转化成协议可传送的报文发送到应用服务器；

5）应用服务器以多线程的方式对客户端的所有请求分别响应；

6）应用服务器分析接收到的报文信息，并调用网络管理通信协议的应用程序接口；

7）应用服务器通过网络管理协议完成与被管对象的消息交互，并将结果通过网络管理通信协议的应用程序接口和流处理器返回客户端。

本发明的网络管理方法增强了互联网环境中被管理设备的安全性。

改进后的客户端通过使用不同的协议处理器就可以使用不同的通信协议，这些协议处理器都是可以自定义和互换的。这对于不同的用户需求和环境要求都有非常好的灵活性。能够使互联网客户端可以通过防火墙访问到内部网络中的设备代理。

附图说明：

图 1 是本发明网络管理系统的总体结构图；

图 2 是本发明网络管理方法的原理图；

图 3 是本发明网络管理方法中的客户端通信处理流程图；

图 4 是本发明网络管理方法中的应用服务器处理流程图；

图 5 是本发明的网络管理系统应用的组网示意图；

具体实施方式：

下面结合图 1 进一步详细说明本发明的网络管理系统：

如图 1 所示的系统结构图，本发明的网络管理系统采用三层体系结构，将三层体系结构进行如下的划分：

客户端 11 为第一层，即表示层；第二层为应用服务器 12；第三层为被管对象 13。客户端 11 可以经过防火墙与应用服务器 12 通信。应用服务器 12 和被管理对象 13 都在安全网络环境中，通信使用的是现有的网络管理通信协议如：SNMP、电信网管协议、Q3 协议等等，图 1 中以 SNMP 为例。

客户端 11 与应用服务器 12 之间的通信协议可以采用适合于互联网环境的通信协议。如：HTTP 协议、简单邮件传输协议、网络新闻传输协议、简单对象访问协议 SOAP 等等，图 1 中以 HTTP 协议为例。信息的载体可以使用简单的文本

或者使用 XML 文件格式。

应用服务器 12 除了分别完成与客户端 11 和被管理对象 13 之间的通信外，还要解析客户端 11 的请求，并转化为相应的网络管理协议的请求。除了与被管理对象 13 之间进行交互外，还要将相关数据转化为相应的报文发送回客户端 11。

下面就针对客户端与服务器端采用 HTTP 协议通信，服务器端和管理对象采用 SNMP 协议的典型案例进行论述。

系统组成：

应用服务器 12 主要是由 Servlet（服务器端动态页面）引擎 23 构成，实现动态服务端的 WWW 服务；还包括 SNMP API（SNMP 应用程序接口）24，用于实现 SNMP 通信。

被管理的对象 13 可以是任何支持 SNMP 的设备代理 25。

参考图 2 所示的网络管理方法原理图，客户端 11 的相关请求通过 HTTP 协议处理器 21 和中间层的 WEB 应用服务器 12 通信。应用服务器 12 解析 HTTP 头部信息，将客户端 11 的请求转化为 SNMP 的相关参数，并负责将请求发送到被管设备的代理 25 以及接收响应信息，再通过 HTTP 返回响应给客户端 11。

从上面可以看出，通信过程是比较复杂的。为了简化应用程序客户端的处理难度，需要将通信过程与内容分开处理。内容的处理与相应的业务相关，对于不同的设备其处理过程千差万别，在这里不做讨论。在这里着重讨论通信的处理。为了可以处理多种协议的通信，提出了协议处理器的概念。因为不同协议的通信过程是完全不同的，所以可以根据不同的通信协议开发不同的协议处理器，然后在软件开发中业务开发人员根据不同的情况选用不同的协议处理器即可。这样，业务逻辑开发人员就可以和通信软件开发者分工合作了。业务逻辑开发人员只注重于业务，即通信内容的处理；协议处理器开发人员只关心通信协议细节的处理。

在 Java 语言的核心库中，已经包含了许多常用的协议处理器，如：FTP、TELNET、HTTP 等等。在使用 Java 进行应用程序的开发时可以使用 HTTP 协议处理器。但是， Java 提供的 HTTP 协议处理器处理 HTTP 通信时的效率非常低。因为在 Java 中，数据的返回时需要等待实际通信结束以后，然而在通信过程时间比较长的情况下，客户就需要等待非常长的时间。因此，可以对其进行简化，如：只需要实现 HTTP 协议的 POST 和 GET 方法即可，这样使得服务端响应的

数据能够及时返回。

下面再结合图 3 和 4 详细描述本发明的网络管理方法。

如图 3 所示的客户端通信处理流程，应用程序客户端在和服务端交互之前首先选用协议处理器，这里选用简化的 HTTP 协议处理器来进行处理。通过提供 HTTP 通信协议所需要的相关参数，如：服务器地址、HTTP 端口号等等，协议处理器 21 实例化一个自定义的流处理器 22 返回给客户端。客户端程序需要提供有关 SNMP 操作的相关信息给流处理器 22，如：被管理对象代理的 IP 地址、SNMP 端口号、团体串等等。流处理器 22 和服务端 12 建立 TCP 连接，然后将上述的相关参数转化为 HTTP 报文的形式，发送到服务端。

参考图 4 所示的应用服务器处理流程，应用服务器为了实现 HTTP 服务，使用 Java 的 Servlet 引擎 23 来实现动态的 HTTP 服务。将通常的网络管理信息库 26 查询操作 MIB-Get、MIB-Set、SNMP-Walk、SNMP-GetNext 分别开发了四个通用的 Servlet 类。在启动 WEB-应用服务器的同时启动 Servlet 引擎，服务器就可以进行 HTTP 服务了。服务器的 Servlet 引擎中的 Servlet 被应用程序客户端或者浏览器客户端访问以后就被实例化载入内存中并且开始相应的服务。

服务端的 Servlet 引擎 23 监测到客户端的请求以后，会以多线程的方式调用对应的 Servlet 实例对所有用户的请求做出响应。服务端的 Servlet 实例通过分析 HTTP 请求的参数信息调用 SNMP API 和被管设备代理进行 SNMP 的交互，然后将结果通过 HTTP 发送回客户端。

如图 5 所示的网络管理系统应用的组网示意，在客户端和应用服务器之间安装了一台防火墙服务器。为了安全起见，防火墙不允许互联网和内部网络之间的直接联系。而必须由防火墙服务器来完成代理通信的任务。在这里，代理服务是 HTTP 代理。这个时候客户端选用 HTTP 协议处理器和相应的流处理器。这样，客户端就可以通过防火墙访问到内部网络中的应用服务器了。应用服务器通过对客户端请求的解析，就会选择客户端要求的网络管理协议与对应的设备代理进行通信。并将需要的数据结果返回给客户端。被管对象可以直接为被管设备，也可以通过代理完成对被管设备的网络管理。


客户
端 11
互联网
HTTP
应用
服务
器 12
SNMP
被管
对象
13

图 1

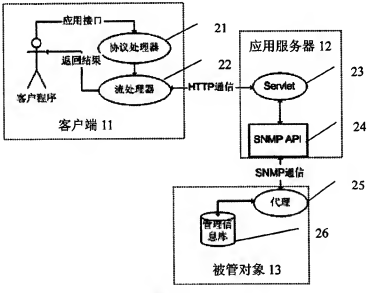
应用接口
协议处理器
返回结果
流处理器
客户程序
客户端 11
21
22
HTTP通信
应用服务器 12
Servlet
23
SNMP API
24
SNMP通信
25
代理
管理信
息库
26
被管对象 13

图 2

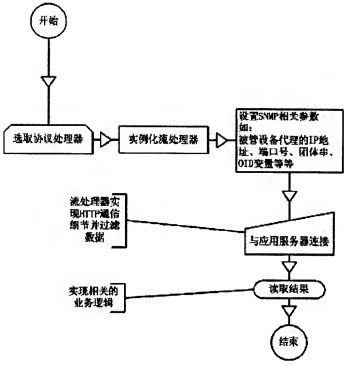
开始
选取协议处理器
实例化该处理器
设置SNMP相关参数
如：
被管设备代理的IP地
址、端口号、团体串、
OID变量等等
流处理器实
现HTTP通信
细节并过滤
数据
与应用服务器连接
实现相关的
业务逻辑
读取结果
结束

图 3

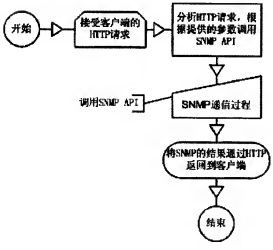
开始
接受客户端的
HTTP请求
分析HTTP请求，根
据提供的参数调用
SNMP API
调用SNMP API
SNMP通信过程
将SNMP的结果通过HTTP
返回到客户端
结束

图 4

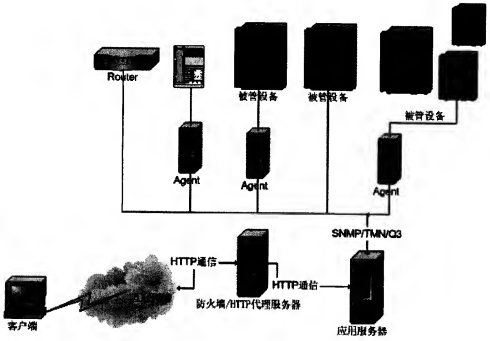
Router
被管设备
被管设备
被管设备
Agent
Agent
Agent
SNMP/TMN/Q3
HTTP通信
HTTP通信
防火墙/HTTP代理服务器
应用服务器
客户端

图 5